Классификация автоматизированных систем по требованиям безопасности информации

Нормативные документы, регламентирующие вопросы аттестации объектов информатизации

- Федеральный закон Российской Федерации от 21 июля 1993 г. № 5485-1 «О государственной тайне»;
- Специальные требования и рекомендации по защите информации, составляющей государственную тайну, от утечки по техническим каналам (СТР). Решение Гостехкомиссии России от 23 мая 1997 г. № 55;
- Положение по аттестации объектов информатизации по требованиям безопасности информации, утвержденное председателем Государственной технической комиссии при Президенте Российской Федерации 25 ноября 1994 г.
- Национальный стандарт РФ ГОСТ РО 0043-003-2012

Документы, регламентирующие классификацию

- -Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации;
- -Защита от несанкционированного доступа к информации. Термины и определения;
- -Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации.

Гриф по заполнении
Экз. №
УТВЕРЖДАЮ
Генеральный директор
_____
_____
«____»_____2014г.

АКТ
классификации автоматизированной системы (АС) «*Наименование*»

Москва «__»_____ 2014 года

Комиссия, назначенная Приказом №_____ от _____г. в составе Председателя комиссии: должность ФИО, членов комиссии: должность ФИО, должность ФИО провела классификацию автоматизированной системы «*Наименование*» и установила:

1. Состав автоматизированной системы объекта информатизации «*Наименование*»

Перечень технических средств автоматизированной системы «*Наименование*» расположенной по адресу: _____:

№	Наименование технического средства АС	Модель, тип	Уч. (зав.) номер
1.			
2.			
3.			
4.			

2. Выявленные определяющие признаки классификации автоматизированной системы:

– Указанная АС не входит в состав локальной сети и не имеет выхода в открытые международные телекоммуникационные сети;

– Наивысший уровень обрабатываемой информации - «_____»;

– Наличие в рассматриваемой автоматизированной системе (АС) информации различного уровня конфиденциальности: «____» ... «____»;

– Уровень полномочий субъектов (пользователей АС) по доступу к защищаемым информационным ресурсам АС;

– Режим работы пользователей АС.

3. Заключение.

Комиссия, учитывая вышеизложенное и рассмотрев следующие утвержденные документы:

• «Перечень защищаемых ресурсов автоматизированной системы «*Наименование*» и уровень их конфиденциальности» (№____ от _____);

• «Перечень лиц, имеющих право самостоятельного доступа к штатным средствам автоматизированной системы «*Наименование*» и уровень их полномочий» (№____ от _____);

• «Матрица доступа субъектов автоматизированной системы «*Наименование*» к ее защищаемым информационным ресурсам» (№__ от _____).

На основании определяющих признаков классификации и в соответствии с п.п. 1.7., 1.9. руководящего документа Гостехкомиссии России «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации» и руководящим документом Гостехкомиссии России «Специальные требования и рекомендации по технической защите информации (СТР)», установила для автоматизированной системы «*Наименование*» класс защищенности ____.

Председатель комиссии:

Члены комиссии:

Автоматизированные системы

Третья группа		Вторая группа		Первая группа				
Однопользова-тельская		Многопользова-тельская с равными полномочиями		Многопользовательская с разными полномочиями				
Уровень конфиденциальности информации								
НС	ОВ, СС, С	НС	ОВ, СС, С	НС	НС	С	СС	ОВ
Классы защищенности								
3Б	**3А**	**2Б**	**2А**	**1Д**	**1Г**	**1В**	**1Б**	**1А**

АС 3А	АС 1А
Подсистема управления доступом	
Должны осуществляться идентификация и проверка подлинности субъектов доступа при входе в систему по паролю длиной не менее шести буквенно-цифровых символов.	Должны осуществляться идентификация и проверка подлинности субъектов доступа при входе в систему по биометрическим характеристикам или специальным устройствам (жетонам, картам, электронным ключам) и паролю временного действия длиной не менее восьми буквенно-цифровых символов
Подсистема регистрации и учета	
Должна осуществляться регистрация входа (выхода) субъектов доступа в систему (из системы), либо регистрация загрузки и инициализации операционной системы и ее программного останова. Регистрация выхода из системы или останова не проводится в моменты аппаратурного отключения АС.	Должна осуществляться регистрация входа (выхода) субъектов доступа в систему (из системы), либо регистрация загрузки и инициализации операционной системы и ее программного останова. Регистрация выхода из системы или останов не проводится в моменты аппаратурного отключения АС. (регистрация производится всех действий пользователя: обращение к подсистеме вывода, обращение к файлам)
Криптографическая подсистема	
Требования не предъявляются	Должно осуществляться шифрование всей информации, записываемой на совместно используемые различными субъектами доступа (разделяемые) носители данных, в каналах связи, а также на любые съемные носители данных (дискеты, микрокассеты и т.п.) долговременной внешней памяти для хранения за пределами сеансов работы санкционированных субъектов доступа. При этом должна выполняться автоматическая очистка областей внешней памяти, содержавших ранее незашифрованную информацию;
Подсистема обеспечения целостности	
Должна быть обеспечена целостность программных средств СЗИ НСД, обрабатываемой информации, а также неизменность программной среды	Должны быть обеспечена целостность программных средств СЗИ НСД, а также неизменность программной среды

Средства защиты от несанкционированного доступа

№	Характеристика	Dallas Lock 8.0-C	Dallas Lock 7.7	Secret Net 7	Secret Net 6.5	«Аккорд-Win32/64»	«Блок хост-сеть К»	«Страж NT 3.0»
1	Производитель	Конфидент		Информзащита		АКБ САПР	Газ-информ-сервис	Модуль
2	Сертификат ФСТЭК (номер, действительно до)	2945 до 16.08.16	2209 до 19.11.16	2707 до 07.09.15	2228 до 03.12.16	2398/ 2400 до 10.08.17	2766 до 29.11.15	2145 до 30.07.16
3	Класс защищенности (РД СВТ Защита от НСД к информации. Показатели защищенности от НСД к информации)	3	3	3	3	3	3	3
4	Класс АС (РД Автоматизированные системы. Защита от НСД к информации. Классификация АС и требования по защите информации)	До класса 1Б включительно						

Организационная структура системы аттестации объектов информатизации

- - федеральный орган по сертификации средств защиты информации и аттестации объектов информатизации по требованиям безопасности информации - ФСТЭК (Гостехкомиссией) России;
- - органы по аттестации объектов информатизации по требованиям безопасности информации;
- - испытательные центры (лаборатории) по сертификации продукции по требованиям безопасности информации;
- - заявители (заказчики, владельцы, разработчики аттестуемых объектов информатизации).

Подготовка АС к аттестации (действия заявителя)

- - проводят подготовку объекта информатизации для аттестации путем реализации необходимых организационно-технических мероприятий по защите информации;
- - привлекают органы по аттестации для организации и проведения аттестации объекта информатизации;
- - предоставляют органам по аттестации необходимые документы и условия для проведения аттестации;
- - привлекают, в необходимых случаях, для проведения испытаний не сертифицированных средств защиты информации, используемых на аттестуемом объекте информатизации, испытательные центры (лаборатории) по сертификации;
- - осуществляют эксплуатацию объекта информатизации в соответствии с условиями и требованиями, установленными в "Аттестате соответствия"(ПРЕДПИСАНИЕ);
- - извещают орган по аттестации, выдавший "Аттестат соответствия", о всех изменениях в информационных технологиях, составе и размещении средств и систем информатики, условиях их эксплуатации, которые могут повлиять на эффективность мер и средств защиты информации (перечень характеристик, определяющих безопасность информации, об изменениях которых требуется обязательно извещать орган по аттестации, приводится в "Аттестате соответствия");
- - предоставляют необходимые документы и условия для осуществления контроля и надзора за эксплуатацией объекта информатизации, прошедшего обязательную аттестацию.

Организационно-распорядительные документы, представляемые организацией для проведения аттестации

- - Технический паспорт на ОВТ (ВП);
- - Приказ об организации работ по защите информации ОВТ (ВП);
- - Инструкция ответственному по защите информации (объекта информатизации (ОИ);
- - Перечень защищаемых сведений, подлежащих обработке на ОВТ (ВП);
- - Перечень ОВТ (ВП);
- - Схема контролируемой зоны организации;
- - Акт категорирования ОВТ (ВП);
- - Описание технологического процесса обработки информации ОВТ;
- - Акт классификации ОВТ;
- - Инструкция администратору безопасности информации ОВТ;
- - Журнал учета персональных паролей ОВТ;
- - Список сотрудников, имеющих право доступа в помещение ОВТ (ВП);
- - Разрешительная система доступа к ресурсам ОВТ;
- - Инструкция пользователя ОВТ;
- - Инструкция по антивирусному контролю ОВТ;
- - Инструкция ответственному за эксплуатацию ОВТ (ВП);
- - Данные по уровню подготовки сотрудников, обеспечивающих защиту информации;
- - Приказ о вводе в эксплуатацию ОИ.

Основные виды работ при аттестации АС

- - анализ исходных данных по аттестуемой АС;
- - предварительное ознакомление с аттестуемой АС;
- - проведение экспертного обследования АС и анализ разработанной документации по защите информации на этом объекте с точки зрения ее соответствия требованиям нормативной и методической документации;
- - проведение испытаний отдельных средств и систем защиты информации на аттестуемой АС с помощью специальной контрольной аппаратуры и тестовых средств;
- - проведение испытаний отдельных средств и систем защиты информации в испытательных центрах (лабораториях) по сертификации средств защиты информации по требованиям безопасности информации;
- - проведение комплексных аттестационных испытаний АС в реальных условиях эксплуатации;
- - анализ результатов экспертного обследования и комплексных аттестационных испытаний АС и утверждение заключения по результатам аттестации.

Спасибо за внимание!